IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

CARLOS RAMIREZ, *on behalf of himself and all others similarly situated*,	*	
Plaintiff,	*	
v.	*	1:21-CV-03758-ELR
THE PARADIES SHOPS, LLC, *a Georgia limited liability company*,	*	
Defendant.	*	

O R D E R

Presently before the Court is Defendant The Paradies Shops, LLC's "Motion to Dismiss the Complaint." [Doc. 8]. For the reasons set forth below, the Court grants Defendant's motion.

I. Background

This putative class action arises from a data breach in which a ransomware attack on Defendant allegedly exposed Plaintiff Carlos Ramirez's name and social security number. See generally Compl. [Doc. 1]. Defendant operates retail stores, restaurants, and bars in airports throughout the United States and Canada. See id. ¶¶ 2, 26. From 2007 to 2014, Plaintiff was an employee of Hojeij Branded Foods ("HBF"). Id. ¶ 61. As a condition of his employment, Plaintiff disclosed to HBF

his name and social security number. Id. In November 2018, Defendant acquired HBF. Id. ¶ 62. In the process of that acquisition, Defendant also obtained personally identifiable information ("PII") of former HBF employees, including Plaintiff's name and social security number. Id.

From October 8–13, 2020, an unauthorized actor purportedly accessed Defendant's "internal administrative system" and uploaded personnel information records to third party servers (the "Data Breach"). See id. ¶ 3; [see also Doc. 1-1]. According to Plaintiff, a Rhode Island state agency informed him by a letter dated February 5, 2021, that someone made a claim for pandemic-related unemployment assistance in his name. Compl. ¶ 64. Plaintiff represents that he received a similar letter from the Kentucky Office of Unemployment Insurance on May 5, 2021. Id. ¶ 65. Plaintiff maintains that he did not make either unemployment application and that whoever submitted the claims would have needed his social security number to do so. Id. ¶¶ 64–65. Thereafter, by a letter dated June 30, 2021, Defendant notified Plaintiff of the Data Breach, informing him that his name and social security number may have been exposed. See id. ¶ 66; [see also Doc 1-1].

II. Procedural History

As a result of these alleged events, Plaintiff initiated this action on September 10, 2021. See generally Compl. In his Complaint, Plaintiff alleges that Defendant failed to adequately protect his and the putative class members' PII and also failed

to promptly notify them of the Data Breach. See, e.g., id. ¶¶ 79, 102, 108, 110, 127. Therefore, Plaintiff brings two (2) Counts against Defendant: Count I—Negligence and Count II—Breach of Implied Contract.[1] Id. ¶¶ 90–131. In support, Plaintiff claims that the Data Breach harmed him because (1) the breach purportedly put him at an "increased risk of fraud, identity theft, and misuse [of his PII]"; (2) he allegedly lost time monitoring his personal and financial records and verifying the legitimacy of Defendant's letter notifying him of the Data Breach; and (3) his PII supposedly decreased in value. See id. ¶¶ 14, 70–72. Lastly, Plaintiff seeks to recover damages and to compel Defendant to adopt more robust information security practices. See id. at 46–50.

On October 4, 2021, Defendant filed its "Motion to Dismiss the Complaint." [Doc. 8]. By its instant motion, Defendant argues that this Court lacks subject matter jurisdiction (based on Plaintiff's purported lack of Article III standing), and further, that Plaintiff fails to state a claim. [See generally id.] On October 11, 2021, Plaintiff submitted an "Unopposed Motion for Extension of Time for Plaintiff's Response to Motion to Dismiss Complaint and Defendant's Reply Thererto," which the Court granted on October 12, 2021, extending Plaintiff's response deadline until October 25, 2021 and Defendant's reply deadline through November 15, 2021. [Docs. 10,

[1] Originally, Plaintiff brought four (4) Counts against Defendant: Count I—Negligence, Count II—Breach of Implied Contract, Count III—Invasion of Privacy, and Count IV—Breach of Confidence. See Compl. ¶¶ 90–157. However, as discussed further below, Plaintiff subsequently withdrew his claims for invasion of privacy and breach of confidence. [See Doc. 12 at 19].

11]. On October 25, 2021, Plaintiff timely filed his response in opposition to Defendant's motion to dismiss. [Doc. 12]. Defendant replied on November 15, 2021. [Doc. 14].

Having been fully briefed, Defendant's motion is now ripe for the Court's review. [Doc. 8]. Because Defendant seeks to dismiss Plaintiff's Complaint pursuant to both Rule 12(b)(1) based on lack of subject matter jurisdiction and Rule 12(b)(6) for failure to state a claim, the Court first addresses the issue of subject matter jurisdiction.

III. Motion to Dismiss Pursuant to Rule 12(b)(1)

Defendant argues that the Complaint should be dismissed because the Court lacks subject matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1) based on Plaintiff's supposed lack of standing to assert his claims. [See id.] The Court examines this argument after setting forth the relevant legal standard.

A. Legal Standard

Federal Rule of Civil Procedure 12(b)(1) permits dismissal of a complaint for lack of subject matter jurisdiction. See FED. R. CIV. P. 12(b)(1). "When a defendant challenges a plaintiff[']s standing by bringing a Rule 12(b)(1) motion, the plaintiff bears the burden to establish that jurisdiction exists." McCabe v. Daimler Ag, No. 1:12-cv-2494-MHC, 2015 WL 11199196, at *2 (N.D. Ga. Aug. 19, 2015).

A defendant may challenge a district court's subject matter jurisdiction through two (2) different types of attacks: facial attacks and factual attacks. See Stalley ex rel. U.S. v. Orlando Reg'l Healthcare Sys., Inc., 524 F.3d 1229, 1232 (11th Cir. 2008). A facial attack on the complaint requires the court "merely to look and see if the plaintiff sufficiently alleged a basis of subject matter jurisdiction, and the allegations in [the] complaint are taken as true for the purposes of the motion." See id. at 1233 (internal quotation omitted). "When defending against a facial attack, the plaintiff has 'safeguards similar to those retained when a Rule 12(b)(6) motion to dismiss for failure to state a claim is raised,' and 'the court must consider the allegations in the plaintiff's complaint as true.'" See id. (quoting McElmurray v. Consol. Gov't of Augusta–Richmond Cnty., 501 F.3d 1244, 1250 (11th Cir. 2007)).

"By contrast, a factual attack on a complaint challenges the existence of subject matter jurisdiction using material extrinsic from the pleadings, such as affidavits or testimony." See id. (internal citation omitted). When assessing a factual attack, the trial court

> may proceed as it never could under 12(b)(6) or FED. R. CIV. P. 56. Because at issue in a factual 12(b)(1) motion is the trial court's jurisdiction—its very power to hear the case—there is substantial authority [in] that the trial court is free to weigh the evidence and satisfy itself as to the existence of its power to hear the case. In short, no presumptive truthfulness attaches to plaintiff's allegations, and the existence of disputed material facts will not preclude the trial court from evaluating for itself the merits of jurisdictional claims.

See Morrison v. Amway Corp., 323 F.3d 920, 925 (11th Cir. 2003) (internal quotation omitted).

B. Discussion

In the matter at bar, Defendant lodges a facial attack on the Complaint, arguing that Plaintiff lacks standing because his allegations fail to present a justiciable controversy as required by Article III of the Constitution. [See Doc. 8-1 at 1]. Article III permits federal courts to adjudicate only "cases" and "controversies." See Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1337 (11th Cir. 2021); see also U.S. CONST. art. III, § 2. It is well-settled that "[t]o satisfy the 'case' or 'controversy' requirement, a plaintiff in a matter must have standing." Tsao, 986 F.3d at 1337. Specifically, to establish Article III standing, a plaintiff must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." Id. (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992)).

Here, Defendant maintains that Plaintiff fails to satisfy the first element of standing: injury in fact.[2] [See Doc. 8-1 at 8–11]. As the Supreme Court has instructed, "[t]o establish injury in fact a plaintiff must show that he or she suffered

[2] Defendants only challenge Plaintiff's standing based on the first element of the Article III standard and do not contest the second or third elements (that an injury be fairly traceable to Defendant's challenged conduct and redressable by a court order). [See Doc. 8-1 at 8–11]; see also Tsao, 986 F.3d at 1337.

'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" Spokeo, Inc. v. Robins, 578 U.S. 330, 339 (2016) (quoting Lujan, 504 U.S. at 560). "For an injury to be particularized, it must affect the [p]laintiff in a personal and individual way." Id. (internal quotation omitted). For an injury to be concrete, it must be "real," not "abstract." Id. at 340. However, intangible injuries—such as the threat of future harm—may be concrete in some circumstances. Id. In particular, such an intangible or threatened injury must be "certainly impending" or, at the very least, pose a "substantial risk" of harm. Tsao, 986 F.3d at 1338–39 (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013)). Allegations that a future injury is merely *possible* "are not sufficient." Clapper, 568 U.S. at 409.

Plaintiff asserts that he has suffered an injury in fact because he now faces an increased risk of future identity theft and because someone used his social security number to make two (2) fraudulent claims for pandemic-related unemployment assistance. [See Doc. 12 at 5–19]. Regarding Plaintiff's first purported injury, his increased risk of future identity theft, Defendant argues that this is insufficient to support Article III standing based on the Eleventh Circuit's recent holding in Tsao. [See Doc. 8-1 at 2, 7] (citing 986 F.3d at 1344). In Tsao, a defendant restaurant chain suffered a data breach leading to the potential exposure of customers' credit card information. Id. at 1334–35. The plaintiff, a customer whose information was

exposed, alleged that he suffered an increased risk of future identity theft as a result of the breach. Id. at 1335. However, the plaintiff in Tsao did not allege any *specific* instance of someone misusing his credit card information. Id. at 1336.

Thus, the Eleventh Circuit explained that "without specific evidence of *some* misuse of class members' data, a named plaintiff's burden to plausibly plead factual allegations sufficient to show that the threatened harm of future identity theft was 'certainly impending'—or that there was a 'substantial risk' of such harm—will be difficult to meet." Id. at 1344 (emphasis in original). Therefore, the Appellate Court found that the plaintiff's "vague, conclusory allegations" of misuse were insufficient to confer standing. Id. at 1343. Additionally, the Court held that "[e]vidence of a mere data breach does not, standing alone, satisfy the requirements of Article III standing." Id. at 1344.

However, the Court finds this case to be distinguishable from Tsao because Plaintiff offers more than "vague, conclusory allegations" of misuse of his PII. See id. at 1343; see also Compl. ¶¶ 64–65. While the plaintiff in Tsao did not allege "any actual misuse of [his] personal data," in the Complaint at hand, Plaintiff alleges two (2) specific instances of someone misusing his social security number. See Compl. ¶¶ 64–65. Specifically, Plaintiff alleges that during February and May of 2021, an unidentified individual made fraudulent claims for pandemic-related unemployment assistance in his name through both the Rhode Island Department of

Labor and Training and the Kentucky Office of Unemployment Insurance. See id. Importantly, Plaintiff alleges that whoever made these claims would have needed his social security number—a critical piece of PII that was allegedly exposed in the Data Breach during October 2020. See id.

In its instant motion, Defendant argues that Plaintiff "has not alleged any facts making it plausible that the [allegedly fraudulent claims for unemployment assistance] he complains of resulted from the attack on [Defendant]" because he does not specifically allege that the person(s) who purportedly made the fraudulent claims in his name acquired his PII as a result of the Data Breach. [See Docs. 8-1 at 9–10; 14 at 6]. However, in considering a motion to dismiss for lack of standing, the Court "accept[s] as true the allegations in the complaint and . . . draws all reasonable inferences in favor of the plaintiff[]." Glynn Env't Coal., Inc. v. Sea Island Acquisition, LLC, 26 F.4th 1235, 1240 (11th Cir. 2022). "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss [the court] presume[s] that general allegations embrace those specific facts that are necessary to support the claim." Lujan, 504 U.S. at 561 (internal quotation omitted).

Here, although Plaintiff does not specifically allege that the person(s) who made fraudulent claims in his name acquired his social security number from the October 2020 Data Breach, he alleges that his social security number was exposed

in the Data Breach and that it was used shortly thereafter to make two (2) fraudulent claims for pandemic-related unemployment assistance. See Compl. ¶¶ 64–65. In drawing all reasonable inferences in favor of the Plaintiff, the Court "presume[s] that [his] general allegations embrace those specific facts that are necessary to support [his] claim[s]"—that is, that Plaintiff's PII was misused in February and May of 2021 as a result of the October 2020 Data Breach. See Lujan, 504 U.S. at 561; see also Glynn Env't Coal, 26 F.4th at 1240.

Thus, the Court finds that Plaintiff has alleged sufficient facts to support a plausible claim that the Data Breach caused him a concrete, particularized, and actual injury when the two (2) fraudulent applications for pandemic-related unemployment assistance were submitted in his name without his knowledge. See Spokeo, 578 U.S. at 339; see also Lujan, 504 U.S. at 560. Therefore, at this juncture, the Court finds that Plaintiff satisfies the injury requirement for standing. See In re Equifax Inc. Customer Data Sec. Breach Litig., 999 F.3d 1247, 1263 (11th Cir. 2021) (quoting Tsao, 986 F.3d at 1340) ("'some allegations of actual misuse or actual access to personal data' support Article III standing"); see also Tsao, 986 F.3d at 1340 ("[T]he cases conferring standing after a data breach based on an increased risk of theft or misuse include[] at least some allegations of actual misuse or actual access to personal data."); accord Hutton v. Nat'l Board of Exam'rs in Optometry, Inc., 892 F.3d 613, 622 (4th Cir. 2018) (finding that fraudulent use or attempted misuse of PII

exposed in a data breach is a concrete injury sufficient to confer standing). And, as noted above, Defendants do not challenge Plaintiff's standing based on either of the other elements required by Article III. See Tsao, 986 F.3d at 1337. Accordingly, the Court rejects Defendant's argument that subject matter jurisdiction is lacking pursuant to Rule 12(b)(1).[3] [Doc. 8].

IV. Motion to Dismiss Pursuant to Rule 12(b)(6)

Having rejected Defendant's argument pursuant to Rule 12(b)(1), the Court now examines Defendant's arguments in favor of dismissal pursuant to Rule 12(b)(6) and Plaintiff's opposition thereto. [Docs. 8-1, 12, 14]. The Court begins by setting forth the relevant legal standard.

A. Legal Standard

When considering a 12(b)(6) motion to dismiss, the Court must accept as true the allegations set forth in the complaint, drawing all reasonable inferences in the light most favorable to the plaintiff. See Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555–56 (2007); U.S. v. Stricker, 524 F. App'x 500, 505 (11th Cir. 2013) (per curiam). Even so, a complaint offering mere "labels and conclusions" or "a formulaic recitation of the elements of a cause of action" is insufficient. See Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Twombly, 550 U.S. at 555);

[3] The Court notes that Defendant's reliance on TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021), is misplaced. Unlike the plaintiffs in that case, Plaintiff in the matter at bar alleges the risk of harm did in fact materialize. See Compl. ¶¶ 64–65.

accord Fin. Sec. Assurance, Inc. v. Stephens, Inc., 500 F.3d 1276, 1282–83 (11th Cir. 2007). Rather, "a pleading must contain a short and plain statement of the claim showing that the pleader is entitled to relief" so as to satisfy "the pleading requirements of Rule 8." See Parker v. Brush Wellman, Inc., 377 F. Supp. 2d 1290, 1294 (N.D. Ga. 2005) (citing FED. R. CIV. P. 8(a)(2)).

Additionally, to survive a Rule 12(b)(6) motion to dismiss, the complaint must "contain sufficient factual matter, accepted as true, 'to state a claim to relief that is plausible on its face.'" See Iqbal, 556 U.S. at 678 (citing Twombly, 550 U.S. at 570). Put differently, a plaintiff must plead "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." See id. This so-called "plausibility standard" is not akin to a probability requirement; rather, the plaintiff must allege sufficient facts such that it is reasonable to expect that discovery will lead to evidence supporting the claim. See id.

B. Discussion

Having set forth the relevant legal standard, the Court now examines the substance of the Parties' arguments. As a preliminary matter, the Court notes that Plaintiff "withdraws his invasion of privacy and breach of confidence claims (Counts III and IV)" in his response brief and makes no arguments in support those

claims. [See Doc. 12 at 20]. Thus, the Court deems these claims abandoned.[4] See Baker v. DeKalb Cnty., No. 1:12-cv-3247-WSD, 2014 WL 793527, at *6 n.13 (N.D. Ga. Feb. 27, 2014) (citation and internal marks omitted) ("Failure to respond to an opposing party's arguments regarding a claim constitutes abandonment of that claim and warrants dismissal of the abandoned claim."). Therefore, the Court assesses Defendant's instant motion as it applies to Plaintiff's two (2) remaining Counts, both of which stem from state law: Count I—Negligence and Count II—Breach of Implied Contract. See Compl. ¶¶ 90–131.

1. Count I—Negligence

In Count I of the Compliant, Plaintiff asserts a claim for negligence. See id. ¶¶ 90–124. Defendant moves to dismiss Plaintiff's negligence claim on the bases that Plaintiff fails to allege (1) the existence of a duty and (2) causation. [See Doc. 8-1 at 12–16]. The Court begins with Defendant's first argument—that Plaintiff does not allege facts to support that Defendant owed him a duty of care. [See id. at 13].

Pursuant to Georgia law, "a negligence claim has four elements: 'the existence of a duty on the part of the defendant, a breach of that duty, causation of the alleged injury, and damages resulting from the alleged breach of the duty.'" Purvis v.

[4] Accordingly, the Court denies Defendant's motion to dismiss as moot as it pertains to Plaintiff's abandoned claims. [Doc. 8].

Aveanna Healthcare, LLC, 563 F. Supp. 3d 1360, 1366 (N.D. Ga. 2021) (quoting Rasnick v. Krishna Hosp., Inc., 713 S.E.2d 835, 837 (Ga. 2011)). "The threshold issue in any cause of action for negligence is whether, and to what extent, the defendant owes the plaintiff a duty of care." City of Rome v. Jordan, 426 S.E.2d 861, 862 (Ga. 1993)).

Plaintiff alleges that Defendant had a duty "to exercise reasonable care in safeguarding, securing, and protecting" Plaintiff's PII because the risk of a data breach and subsequent injury to Plaintiff was "reasonably foreseeable, particularly in light of Defendant's inadequate security practices." See Compl. ¶¶ 95–102. Defendant argues that it had no such duty because the Georgia Supreme Court has "rejected the notion of 'a general legal duty to all the world not to subject others to an unreasonable risk of harm,' including with respect to personal information." [Doc. 8-1 at 13] (quoting Dept. of Labor v. McConnell, 828 S.E.2d 352, 358 (Ga. 2019)). In response, Plaintiff argues that despite the Georgia Supreme Court's opinion in McConnell, "Defendant[] owed a legal duty of care to [Plaintiff] to take reasonable precautions due to the reasonably foreseeable risk of danger of a data breach incident." [Doc. 12 at 22] (internal quotation omitted).

In McConnell,

> a plaintiff filed a class action lawsuit against the Georgia Department of Labor after one of the Department's employees inadvertently sent an email that included a spreadsheet containing the private information of individuals who had applied for unemployment benefits and other

> services from the Department. [McConnell,] 828 S.E.2d at 356. The plaintiff's private information was disclosed through this mistake, and the plaintiff asserted a claim for negligence against the Department. . . .
>
> Ultimately, the Georgia Supreme Court affirmed the Georgia Court of Appeals'[] decision to dismiss the plaintiff's negligence claim, concluding that this claim failed because the plaintiff "has not shown that the Department owed him . . . a duty to protect [his] private information." . . . Specifically, in finding that the plaintiff had failed to show that the Department of Labor owed him and others a duty to protect their personal information, the Georgia Supreme Court merely rejected that such a duty arose from the sources the plaintiff had relied upon to support his claim, namely: (1) the purported duty "to all the world not to subject [others] to an unreasonable risk of harm" that was articulated in Bradley Center v. Wessner, 296 S.E.2d 693 (Ga. 1982); and (2) O.C.G.A. §§ 10-1-910 and 10-1-393.8. Id.

Purvis, 563 F. Supp. 3d at 1367.

Upon review, the Court finds that the matter at bar presents questions of law similar to those addressed by this district in two (2) recent employer data breach cases: Purvis, 563 F. Supp. 3d at 1367, and Sheffler v. Americold Realty Tr., No. 1:21-CV-1075-TCB, 2022 WL 1815505, at *6 (N.D. Ga. Jan. 19, 2022). In Purvis, plaintiffs (including one former employee of the defendant) asserted a negligence claim after a cyberattack on the defendant (a healthcare provider and employer) compromised the plaintiffs' PII. See 563 F. Supp. 3d at 1365. In denying the defendant's motion to dismiss for failure to state a claim, the court examined the consequences of the McConnell decision and concluded that the Georgia Supreme Court "expressly le[ft] open the possibility that a duty to safeguard personal information could still arise under different circumstances and based on different

arguments" than those presented by the plaintiff in McConnell. Id. at 1367. The court found that the plaintiffs in Purvis sufficiently alleged the defendant's duty to safeguard their PII. Id. at 1369. In particular, the court relied on the plaintiffs' allegations that

> [1] the threat of cyberattacks and data breaches was widely and publicly known, especially to healthcare providers such as [d]efendant. . . . [2] that the kind of phishing attack allegedly used in the [d]ata [b]reach is extremely common, and that such attacks can be reasonably guarded against with a variety of preventative measures. . . . [and] [3] that, as a healthcare provider, [d]efendant knew or should have known that it faced a particularly high risk of a data breach but that [d]efendant nevertheless failed to properly guard against this foreseeable risk by implementing reasonable security measures, which ultimately led to [p]laintiffs' injuries as a result of the [d]ata [b]reach.

Id. (internal record citations omitted). Ultimately, the court found that the plaintiffs sufficiently alleged that the "[d]efendant owed them a duty based on [its] alleged knowledge of the foreseeable risk of a data breach and the resulting exposure of [p]laintiffs' information." Id. at 1368.

In contrast, the plaintiff employees in Sheffler asserted a negligence claim against their former employer after a ransomware attack on the employer compromised their PII, including their names and social security numbers. See Sheffler, 2022 WL 1815505, at *1. In granting the defendant employer's motion to dismiss for failure to state a claim, the court found that the plaintiffs' allegations of foreseeability were not as specific as those in Purvis. See id. at *5–6. The court recognized that the plaintiffs alleged "that the harm was foreseeable," that the

defendant "deviated from standard industry rules, regulations, and practices[,] . . . that a breach and injury was reasonably foreseeable in light of [the defendant's] allegedly inadequate security practices[,] and that they were the foreseeable and probable victims." Id. at *5. However, the court distinguished these allegations of foreseeability from those presented by the plaintiffs in Purvis, because those "plaintiffs [specifically] alleged that the attack was foreseeable because the defendant, a healthcare provider, had reason to know that it could be the target of the exact type of breach it experienced," and that "the specific type of phishing attack at issue was very common and could be guarded against." Id. at *6. Thus, the court found that the plaintiffs did "not provide any factual allegations to plausibly support a conclusion that [the defendant] had reason to be on guard for this type of ransomware attack," or that "[the defendant's] type of business had cause to be particularly on guard against such an attack." Id. Therefore, because the allegations of the complaint lacked sufficient specificity, the court found that the plaintiffs in Sheffler failed to allege the defendant's duty to safeguard their PII. Id.

In the matter at bar, the Court finds Plaintiff's allegations regarding foreseeability and duty to be less specific than the plaintiffs' allegations in Purvis. See 563 F. Supp. 3d at 1369; see also Compl. ¶¶ 43–44, 95–102. In contrast to Purvis, Plaintiff does not allege that the threat of cyberattacks and data breaches was especially well-known to Defendant or Defendant's type of business. See 563 F.

Supp. 3d at 1369. Plaintiff does not allege that the particular kind of attack Defendant suffered is extremely common. Id. Further, Plaintiff does not allege that Defendant (either Defendant in particular or by virtue of its industry—airport retail and dining) knew or should have known that it faced a particularly high risk of a data breach. Id.

Moreover, the Court finds Plaintiff's allegations to be very similar—and in some instances, identical—to the insufficient allegations made by the plaintiffs in Sheffler. Here, as in Sheffler, Plaintiff alleges that the defendant "deviated from standard industry rules, regulations, and practices;" that "[a] breach of security . . . and resulting injury to Plaintiff . . . was reasonably foreseeable in light of Defendant's inadequate security practices;" and that Plaintiff was "the foreseeable and probable victim[]." See Compl. ¶¶ 100–01; see also Sheffler, 2022 WL 1815505, at *5. However, as in Sheffler, Plaintiff does not allege that Defendant (either in particular or by virtue of its industry) had reason to know of or guard against the type of ransomware attack it experienced. See Sheffler, 2022 WL 1815505, at *6. Plaintiff makes two (2) allegations that approach this standard, but ultimately fall short. Specifically, Plaintiff alleges—exactly as the plaintiffs in Sheffler did—that:

> [1] Defendant's negligence in safeguarding the PII of Plaintiff . . . is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data[;] and

> [2] Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff . . . from being compromised.

See Compl. ¶¶ 43–44; see also Sheffler, 2022 WL 1815505, at *5–6. The above allegations are insufficient because Plaintiff does not claim that any of these "repeated warnings and alerts" were ever directed specifically toward Defendant or Defendant's type of business. Further, Plaintiff does not allege that Defendant had actual knowledge or any particular reason to be aware of such "public announcements," or that these alleged announcements addressed data breaches involving Defendant's type of business. Thus, in line with the above persuasive authority, the Court finds that Plaintiff fails to sufficiently plead specific factual allegations to establish that Defendant had a duty of care to safeguard Plaintiff's PII.[5] See Sheffler, 2022 WL 1815505, at *5–6.

Because Plaintiff fails to establish the first element necessary to adequately state a claim for negligence, the Court's inquiry as to his Count I need not proceed. Rasnick v. Krishna Hosp., Inc., 713 S.E.2d 835, 837 (Ga. 2011). The Court

[5] Defendant also argues that it had no duty to safeguard Plaintiff's PII because its relationship with Plaintiff was purportedly less direct than the parties' relationship in McConnell. [See Doc. 8-1 at 13]. Specifically, relying on McConnell, Defendant argues that because Plaintiff provided his PII to HBF and not directly to Defendant, Defendant had no duty to safeguard Plaintiff's PII. [See id.] Although it does not alter the Court's above conclusion, the Court rejects this argument by Defendant because the Georgia Supreme Court's reasoning in McConnell had nothing to do with the "directness" of the relationship between the parties. Rather, in McConnell, "the Georgia Supreme Court merely rejected that [a duty to protect PII] arose from the sources the plaintiff had relied upon to support his claim, namely: (1) the purported duty to all the world not to subject [others] to an unreasonable risk of harm . . . and (2) O.C.G.A. §§ 10-1-910 and 10-1-393.8." Purvis, 563 F. Supp. 3d at 1367 (internal citations omitted).

concludes that Plaintiff has not alleged sufficient facts to state a plausible claim for negligence.[6] See Sheffler, 2022 WL 1815505 at *5–6 (granting motion to dismiss on negligence claim because the plaintiff employees' allegations were not sufficiently specific to establish that the defendant had a duty to safeguard their PII). Accordingly, the Court grants Defendant's motion to dismiss as to Plaintiff's Count I—Negligence. [Doc. 8].

2. Count II—Breach of Implied Contract

In Count II of the Compliant, Plaintiff asserts a claim for breach of implied contract. See Compl. ¶¶ 125–31. Defendant argues that Plaintiff purportedly fails to allege any of the claim's elements, including "assent of the parties to the terms of the contract." [See Docs. 8-1 at 16–17; 14 at 11].

Pursuant to Georgia law, "a valid contract requires 'parties able to contract, a consideration moving to the contract, the assent of the parties to the terms of the contract, and a subject matter upon which the contract can operate.'" Purvis, 563 F. Supp. 3d at 1379 (quoting O.C.G.A. § 13-3-1). "Mutual assent, or a meeting of the minds, is the first requirement of the law relative to contracts." Id. (internal quotations omitted). "An implied contract is one not created or evidenced by distinct

[6] Additionally, although the Parties do not address it in their briefs, the Court notes that "Plaintiff[] cannot state a claim under Section 5 of the [Federal Trade Commission ("FTC")] Act. Sheffler, 2022 WL 1815505, at *6. "That law applies to consumers, competitors, or those harmed by destruction of competition." Id. (internal citations omitted). Plaintiff does not cite any authority—nor does the Court locate any—"extending Section 5 of the FTC Act to the employer/employee context." Id.

and explicit language, but inferred by the law as a matter of reason and justice." Classic Restorations, Inc. v. Bean, 272 S.E.2d 557, 562–63 (Ga. Ct. App. 1980). "Contracts implied in fact are inferred from the facts and circumstances of the case[.]" Dawes Mining Co. v. Callahan, 267 S.E.2d 830, 832 (Ga. Ct. App. 1980).

Here, Plaintiff alleges that he provided his name and social security number to "Defendant or a company it acquired" as a condition of his employment, and in doing so, entered an implied contract with Defendant by which it agreed to safeguard Plaintiff's PII. Compl. ¶ 127. However, to survive dismissal, Plaintiff "must allege facts to allow a plausible inference that [Defendant] intended to bind itself to protect . . . [his] information." Sheffler, 2022 WL 1815505, at *6.

Here, Plaintiff alleges that as a condition of his employment with HBF—the company later acquired by Defendant—he was required to "provide and/or entrust his PII" to HBF. Compl. ¶ 61. However, Plaintiff does not allege "facts or circumstances that indicate how Defendant allegedly manifested an intent to provide data security as part of the [P]arties' employment agreement." See Purvis, 563 F. Supp. 3d at 1382; see also Compl. Without more, this allegation is insufficient to support Plaintiff's claim. See Purvis, 563 F. Supp. 3d at 1382 (dismissing employee's implied contract claim); see also Sheffler, 2022 WL 1815505, at *6 (dismissing employees' implied contract claim where the claim was based on "the allegation that [employees] provided their employer . . . with their personal

information to obtain employment."); accord Longenecker-Wells v. Benecard Servs. Inc., 658 F. App'x 659, 662 (3d Cir. 2016) (dismissing employees' implied contract claim and holding that employer's requirement that employees provide PII prior to starting "did not create a contractual promise to safeguard that information").

Thus, the Court finds Plaintiff's allegations insufficient to state a plausible claim for breach of implied contract. See Purvis, 563 F. Supp. 3d at 1379; see also O.C.G.A. § 13-3-1. Therefore, the Court grants Defendant's motion to dismiss as to Plaintiff's Count II. [Doc. 8].

V. Conclusion

For the reasons set forth above, the Court **GRANTS IN PART AND DENIES AS MOOT IN PART** Defendant's "Motion to Dismiss the Complaint." [Doc. 8]. Specifically, the Court **GRANTS** Defendant's motion as to Plaintiff's Count I—Negligence and Count II—Breach of Implied Contract. The Court **DENIES AS MOOT** Defendant's motion as to Plaintiff's abandoned claims, Counts III—Invasion of Privacy and Count IV—Breach of Confidence. Because no claims remain, the Court **DISMISSES** this action and **DIRECTS** the Clerk to **CLOSE** this case.

SO ORDERED, this 27th day of July, 2022.

Eleanor L. Ross
United States District Judge
Northern District of Georgia